The Probabilistic Method

Andreas Klappenecker

Texas A&M University

The Idea

Suppose that we want to prove the **existence** of a combinatorial object that has certain properties.

In the **probabilistic method**, we approach this problem by defining a sample space of combinatorial objects and showing that a randomly chosen element of this space has the desired properties with positive probability.

Ramsey Numbers

The Problem $n = R(a, b)$

What is the **smallest number** $n = R(a, b)$ such that in any set of n people there must be

1. a mutually aquainted people or
2. b mutual strangers.

The numbers $R(a, b)$ are called **Ramsey numbers**.

We can model a set of n people with a complete graph. We color an edge (i, j) **red** if i and j are acquainted and **blue** otherwise.

Reformulated Problem

Let $R(a, b)$ be the smallest integer n such that in any edge-coloring of K_n with the two colors **red** and **blue**, there exists

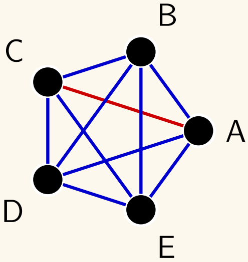
1. an induced **red** K_a subgraph or
2. an induced **blue** K_b subgraph.

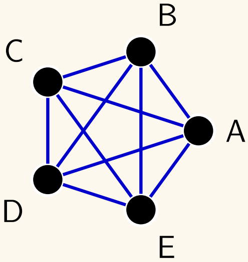
Proposition

$$R(2, n) = n$$

Proof.

This one is easy. Any coloring of K_n has either has (a) one or more red edges, so it contains a red K_2, or (b) it does not contain any red edges, but then it contains a blue K_n.

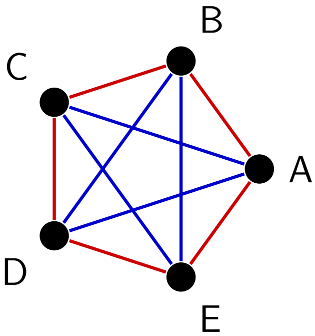




We can also formulate it as follows. At a party with n people, there are either two people knowing each other or they are all mutual strangers. □

Proposition

$R(3,3) > 5$



In a party of 5 people, it can happen that there are no 3 people that are mutually aquainted and no 3 people that are mutually strangers.

Example

Proposition

$R(3, 3) = 6$.

Proof.

It suffices to show that $R(3,3) \leqslant 6$. Let $G = (V, E)$ be the red induced subgraph of K_6. Let $u \in V$ be an arbitrary vertex. Then there are two cases:

1. Suppose that the set $N(u) = \{v \in V | (u, v\} \in E\}$ has at least 3 elements. Then either $N(u)$ is an independent set of strangers and the proposition holds, or we have two adjacent vertices $v_1, v_2 \in N(u)$, in which case $\{u, v_1, v_2\}$ is a clique of friends and the proposition also holds.
2. Suppose that the set $N(u) = \{v \in V | (u, v) \in E\}$ has at most 2 elements. Then by case (1), there is a clique or a independent set of size 3 in the complement graph of G and thus also in G.

In any case, we have that $R(3,3) \leqslant 6$, as claimed. $\square$

Finding the precise value of the Ramsey numbers $R(a, b)$ is at the heart of Ramsey theory in combinatorics.

It is known that K_n contains a red K_a or a blue K_b induced subgraph for all large n, but finding the precise value of $R(a, b)$ is difficult.

$$R(3, 3) = 6, \quad R(4, 4) = 18, \quad R(5, 5) = ?$$

Proposition (Erdős)

If $\binom{n}{k} 2^{1-\binom{k}{2}} < 1$, *then* $R(k,k) > n$.

Proof.

Consider K_n and a random 2-coloring on its edges, namely we color an edge **red** with probability $1/2$, and **blue** with probability $1/2$. For any k-subset S of vertices, let M_S be the event that the induced subgraph on S is monochromatic. Then,

$$\Pr[M_S] = \Pr[S \text{ red}] + \Pr[S \text{ blue}] = \frac{1}{2^{\binom{k}{2}}} + \frac{1}{2^{\binom{k}{2}}} = 2^{1-\binom{k}{2}}.$$

Thus, the probability that some k-subset forms a monochromatic subgraph is at most $\binom{n}{k}2^{1-\binom{k}{2}}$. Since $\binom{n}{k}2^{1-\binom{k}{2}} < 1$, there exists some 2-coloring for which there is no monochromatic K_k. In other words, $R(k,k) > n$. $\square$

Hamiltonian Paths in Tournaments

Tournaments

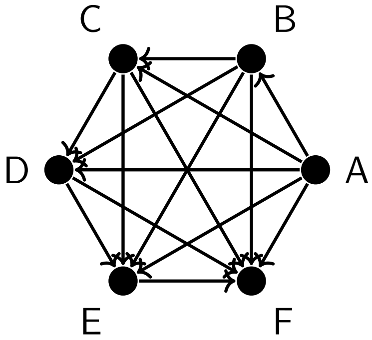
Definition

A **tournament** T_n is a directed graph that is obtained from undirected complete graph K_n by orienting each edge.

The directed graph T_n represents a round robin tournament with n players. An edge (u, v) in the graph T_n means that player u has beaten player v.

Definition

A **Hamiltonian path** is a path of $n-1$ edges that visits each vertex of T_n precisely once, $v_1 \to v_2 \to v_3 \to \cdots \to v_n$.



$$A \to B \to C \to D \to E \to F$$
$$B \to A \to C \to D \to E \to F$$

Our goal is to show that there exists a tournament that has an abundance of Hamiltonian paths.

Proposition

Consider the complete graph K_n on n vertices. There exists a tournament on K_n that has at least $n!/2^{n-1}$ Hamiltonian paths.

Pigeonhole Principle of Expectation

Proposition

A random variable cannot always be less than its expected value.

Pigeonhole Principle of Expectation

Proposition

A random variable cannot always be less than its expected value.

Proof.

Seeking a contradiction, suppose that X is a discrete random variable that has values always less than $\mu = \mathrm{E}[X]$. Then

$$\mathrm{E}[X] = \sum_{\alpha \in X(\Omega)} \alpha \Pr[X = \alpha] < \sum_{\alpha \in X(\Omega)} \mu \Pr[X = \alpha] = \mathrm{E}[X],$$

contradiction. □

Proposition

A random variable cannot always be less than its expected value.

Proof.

Seeking a contradiction, suppose that X is a discrete random variable that has values always less than $\mu = \mathrm{E}[X]$. Then

$$\mathrm{E}[X] = \sum_{\alpha \in X(\Omega)} \alpha \Pr[X = \alpha] < \sum_{\alpha \in X(\Omega)} \mu \Pr[X = \alpha] = \mathrm{E}[X],$$

contradiction. $\square$

Similarly, a random variable cannot always be larger than its expected value.

Proof.

Construct a tournament on K_n by randomly orienting each edge in K_n with probability $1/2$. Consider a random permutation π on n points. The vertices $(v_{\pi 1}, v_{\pi 2}, \ldots, v_{\pi n})$ form a Hamiltonian path if and only if $v_{\pi k}$ beats $v_{\pi(k+1)}$ for all k in the range $1 \leqslant k \leqslant n-1$. Let X_π denote the indicator random variable for the event that π yields a Hamiltonian path. Then

$$\mathrm{E}[X_\pi] = \Pr[X_\pi = 1] = 1/2^{n-1}.$$

Let $X = \sum X_\pi$ be the random variable counting Hamiltonian paths. Since there are $n!$ permutations, the expected number of Hamiltonian paths is

$$\mathrm{E}[X] = \sum_{\pi \in S_n} \mathrm{E}[X_\pi] = n!/2^{n-1}.$$

By the pigeonhole principle of expectation, it follows that some tournament must have at least $n!/2^{n-1}$ Hamiltonian paths.

Large Cuts

Problem

Given an undirected graph G. Find a maximum cut in G.

Problem

Given an undirected graph G. Find a maximum cut in G.

The problem is NP-hard, so there is little hope to find an efficient randomized algorithm to solve it. We can consider a weaker version.

Large Cuts

Problem

Given an undirected graph G. Find a maximum cut in G.

The problem is NP-hard, so there is little hope to find an efficient randomized algorithm to solve it. We can consider a weaker version.

Problem

Given an undirected graph G with m edges. Find a large cut that has at least $m/2$ edges.

Large Cuts

Proposition

Given an undirected graph $G = (V, E)$ with m edges, there exists a partition of V into two disjoint sets A and B such that at least $m/2$ edges cross the cut (A, B).

Proof.

For each vertex, flip a fair coin and put the vertex in A if the coin shows heads, and put the vertex in B if the coin shows tails. Let $e_1, e_2, \ldots, e_m$ be an enumeration of the edges in E. Define the indicator random variable X_k

$$X_k = \begin{cases} 1 & \text{if edge } k \text{ crosses the cut } (A, B), \\ 0 & \text{otherwise} \end{cases}$$

Proof. (Continued)

The probability that the edge crosses the cut (A, B) is $1/2$; hence,

$$E[X_k] = \frac{1}{2}.$$

Let $S(A, B)$ denote the size of the cut (A, B). Then

$$E[S(A, B)] = E\left[\sum_{k=1}^{m} X_k\right] = \sum_{k=1}^{m} E[X_k] = \frac{m}{2}.$$

Thus, there exists a cut (A, B) of size $m/2$. $\square$

Probabilistic Circuits

Probabilistic Circuits

Definition

A **probabilistic circuit** has n standard input variables $x_1, \ldots, x_n$ and m random inputs. The random inputs are chosen uniformly at random from $\{0, 1\}$.

We say that $C(x)$ computes are boolean function $f \colon \{0, 1\}^n \to \{0, 1\}$ if and only if

$$\Pr[C(x) = f(x)] \geqslant 3/4$$

holds for all inputs $x \in \{0, 1\}^n$.

In other words, $C(x)$ is a boolean circuit that has access to m coin flips.

Question

Can probabilistic circuits for computing a boolean function $f(x)$ have a much smaller circuit size than deterministic circuits?

Definition

The **majority function** Maj_n on n boolean variables is defined as

$$\mathrm{Maj}_n(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } x_1 + x_2 + \cdots + x_n \geqslant \lceil n/2 \rceil, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition

Let $X_1, X_2, \ldots, X_m$ be independent Bernoulli random variables with

$$\Pr[X_k = 1] = 1/2 + \epsilon$$

for all k in the range $1 \leqslant k \leqslant m$. Then

$$\Pr[\mathrm{Maj}(X_1, X_2, \ldots, X_m) = 0] \leqslant e^{-2\epsilon^2 m}.$$

Proof.

Let $\mathcal{F}$ be the family of all subsets of $\{1, 2, \ldots, m\}$ of size $\geqslant \lceil m/2 \rceil$.
Let us denote the probability

$$\Pr[\mathrm{Maj}(X_1, X_2, \ldots, X_m) = 0]$$

that most random variables have the value 0 shortly by q.
We can express q explicitly as follows:

$$\begin{aligned} q &= \sum_{S \in \mathcal{F}} \Pr[X_k = 0 \text{ for all } k \in S] \Pr[X_k = 1 \text{ for all } k \notin S] \\ &= \sum_{S \in \mathcal{F}} (1/2 - \epsilon)^{|S|} (1/2 + \epsilon)^{m - |S|} \end{aligned}$$

Proof. (Continued)

If we multiply each term of the latter sum by the factor

$$\left(\frac{1/2+\epsilon}{1/2-\epsilon}\right)^{|S|-m/2} \geqslant 1,$$

then we get the bound

$$\begin{aligned} q &= \sum_{S\in\mathcal{F}} (1/2-\epsilon)^{|S|}(1/2+\epsilon)^{m-|S|} \\ &\leqslant \sum_{S\in\mathcal{F}} (1/2-\epsilon)^{m/2}(1/2+\epsilon)^{m/2}. \end{aligned}$$

Proof. (Continued)

Since $\mathcal{F}$ contains at most 2^m sets, we can rewrite the sum as

$$
\begin{aligned}
q &\leqslant \sum_{S \in \mathcal{F}} (1/2 - \epsilon)^{m/2} (1/2 + \epsilon)^{m/2} \\
&\leqslant 2^m (1/2 - \epsilon)^{m/2} (1/2 + \epsilon)^{m/2} \\
&= (1 - 2\epsilon)^{m/2} (1 + 2\epsilon)^{m/2} \\
&= (1 - 4\epsilon^2)^{m/2} \leqslant e^{-4\epsilon^2 m/2} = e^{-2\epsilon^2 m},
\end{aligned}
$$

which proves the claim.

Proposition (Adelman)

If a boolean function f of n variables can be computed by a probabilistic circuit of size M, then f can be computed by a deterministic circuit of size at most $8nM$.

Proof

Let C be a probabilistic circuit that computes f.

Take m independent copies of $C_1, C_2, \ldots, C_m$ of C with their own independent random inputs.

Let C' denote the probabilistic that computes the majority of the results of the m copies,

$$C'(x) = \mathrm{Maj}(C_1(x), C_2(x), \ldots, C_m(x)).$$

Proof. (Continued)

Fix an input $v \in \mathbf{F}_2^n$. Let X_k denote the indicator random variable for the event

$$C_k(v) = f(v).$$

Then $\Pr[X_k = 1] = 1/2 + \epsilon$ with $\epsilon = 1/4$.

Since C' uses majority logic, it will err with probability

$$\Pr[C'(v) \neq f(v)] \leqslant e^{-2\epsilon^2 m} = e^{-m/8}.$$

By the union bound, C' will err for some input with probability

$$\Pr[\exists v \in \mathbf{F}_2^n \colon C'(v) \neq f(v)] \leqslant 2^n e^{-m/8}.$$

Proof. (Continued)

If we choose $m = 8n$, then

$$\Pr[\exists v \in \mathbf{F}_2^n \colon C'(v) \neq f(v)] \leqslant 2^n e^{-n} < 1.$$

We can conclude that there must exist some assignment ν of random inputs such that

$$C'(v) = f(v)$$

for all $v \in \mathbf{F}_2^n$. If we fix the random inputs in C' to the values given in ν, then this is a deterministic circuit of size $8nM$, as claimed.[a]

[a] If we want to be picky, then we should add $O(\log(8n))$ gates to implement the majority logic.

Alterations

Alterations

The Idea

Our goal is to prove the existence of a combinatorial object that has certain properties.

Sometimes we will struggle to show that a randomly chosen element has **all** the desired properties with positive probability. Maybe we will be able to construct a combinatorial object that has **some** of the properties. This is also ok, as long as we can **alter** the combinatorial object into some object that has all the desired properties.

Proposition

For any positive integer n,

$$R(k,k) > n - \binom{n}{k} 2^{1-\binom{k}{2}}.$$

Proof.

Consider a random coloring of the edges of K_n with two colors. We color each edge e independently such that

$$\Pr[e\ \textbf{red}] = \frac{1}{2} = \Pr[e\ \textbf{blue}].$$

For any subset R of the set of vertices with k elements, let X_R denote the indicator random variable for the event that the induced subgraph on R is monochromatic.

Proof. (Continued)

Let
$$X = \sum X_R,$$
where the sum extends over all k-subsets of the vertex set of K_n.
Then
$$\mathrm{E}[X] = \sum \mathrm{E}[X_R] = \binom{n}{k} 2^{1-\binom{k}{2}}.$$
It follows that there exists a 2-coloring that has at most $X \leqslant \binom{n}{k} 2^{1-\binom{k}{2}}$ monochromatic K_k subgraphs.

Proof. (Continued)

If we delete one vertex from each monochromatic subgraph, we obtain a coloring of a complete graph with

$$n - \binom{n}{k} 2^{1-\binom{k}{2}}$$

vertices that does not have any monochromatic K_k subgraphs.
It follows that $R(k,k) > n - \binom{n}{k} 2^{1-\binom{k}{2}}$, as claimed. $\square$

References

1. Noga Alon, Joel H. Spencer, The Probabilistic Method, 2nd edition, Wiley, 2000.
2. Stasys Jukna, Boolean Function Complexity, Springer, 2012.